Claims

What is claimed is:

1. A method of restoring data of a key-server in communication with a communication network comprising the steps of:
providing the key-server in communication with the communication network;
providing to at least a computer in communication with the communication network, a plurality of portable data storage devices each having stored thereon security data relating to a single authorized user;
copying from each of the plurality of portable data storage devices, security data relating to the single authorized user.

2. A method of restoring data of a key-server in communication with a communication network as defined in claim 1 wherein the step of copying comprises the steps of:
forming a secure communication session between at least one of the plurality of portable data storage devices and the key-server;
transferring the security data via the secure communication session from the portable data storage device to the key-server; and,
storing the transferred security data within memory means of the key-server.

3. A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the plurality of portable data storage devices comprise all the security data to be restored in the key-server.

4. A method of restoring data of a key-server in communication with a communication network as defined in claim 3 wherein the plurality of portable data storage devices includes memory having stored therein security data relating to each single authorized user of the communication network.

5. A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the portable data storage device includes a

processor for ciphering data using the security data stored therein and comprising the steps of:

providing cryptographic functions within the portable data storage device using the security data stored therein.

6. A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the key-server includes a processor for ciphering data using the security data stored therein and comprising the steps of:

providing cryptographic functions within the key-server using the security data stored therein.

7. A method of restoring data of a key-server in communication with a communication network as defined in claim 6 comprising the steps of:

determining at least an available user information entry device from a plurality of known user information entry devices;

receiving unique user identification information via the at least an available user information entry device; and,

registering the received user identification information against security data for that user stored in the key-server;

wherein, when the user identification information is indicative of an authorized user the step of ciphering data is performed with security data associated with the authorized user.

8. A method of restoring data of a key-server in communication with a communication network as defined in claim 3 wherein each of the plurality of portable data storage devices are provided at each of a plurality of computers in communication with the network.

9. A method of restoring data of a key-server in communication with a communication network as defined in claim 8 wherein the portable data storage device is one of a token and a smart card.

10. A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the portable data storage device is one of a token and a smart card.

11. A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein at least a portable data storage device provides dedicated cryptographic functions for the at least a computer in communication with the communication network using the security data stored internal to the at least a portable data storage device.

12. A method of restoring data of a key-server in communication with a communication network as defined in claim 11 wherein the security data stored internal to the at least a portable data storage device are not accessible in a useable form from outside of the key-server and the at least a portable data storage device.

13. A method of restoring data of a key-server in communication with a communication network as defined in claim 2 wherein the key-server provides dedicated cryptographic functions for the at least a computer in communication with the communication network using the security data stored internal to the key-server.

14. A method of backing up data of a key-server in communication with a communication network comprising the steps of:

providing the key-server in communication with the communication network, the key-server having stored thereon the unique user identification information for a plurality of authorized users of the communication network and the security data for use by the specific authorized user in accessing data within the network;

providing to at least a computer in communication with the communication network, a portable data storage device;

receiving user identification data indicative of an authorized user of the communication network; and,

copying from the key-server to the portable data storage device, security data relating to the authorized user for use by the specific authorized user in accessing data within the network.

15. A method of backing up data of a key-server in communication with a communication network as defined in claim 14 wherein the step of copying comprises the steps of:

forming a secure communication session between the key-server and the portable data storage device;

transferring the security data relating to a specific authorized user via the secure communication session from the key-server to the portable data storage device assigned to that specific authorized user; and,

storing the transferred security data relating to a specific authorized user within the memory means of the portable data storage device.

16. A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein security data specific to each of a plurality of authorized users of the communication network is stored on a separate portable data storage device assigned uniquely to one of the plurality of authorized users, wherein the security data of the key-server is partially stored within each portable data storage device and wherein all data within the plurality of portable data storage devices is sufficient to restore security data to the key-server in the event of a data loss thereto.

17. A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein the portable data storage device includes a processor for ciphering data using the security data stored therein and comprising the steps of:

providing cryptographic functions within the portable data storage device using the security data stored therein.

18. A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein the key-server includes a processor for ciphering data using the security data stored therein and comprising the steps of:

providing cryptographic functions within the key-server using the security data stored therein.

19. A method of backing up data of a key-server in communication with a communication network as defined in claim 18 comprising the steps of:

determining at least an available user information entry device from a plurality of known user information entry devices;

receiving unique user identification information via the at least an available user information entry device; and,

registering the received user identification information against security data for that user stored in the key-server,

wherein, when the user identification information is indicative of an authorized user, the step of ciphering data is performed with security data associated with the authorized user.

20. A method of backing up data of a key-server in communication with a communication network as defined in claim 16 wherein each of the plurality of portable data storage devices are provided at each of a plurality of computers in communication with the network.

21. A method of backing up data of a key-server in communication with a communication network as defined in claim 20 wherein the portable storage device is one of a smart card and a PCMCIA token.

22. A method of backing up data of a key-server in communication with a communication network as defined in claim 16 wherein the portable storage device is one of a smart card and a PCMCIA token.

23. A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein the portable data storage device provides dedicated cryptographic functions for the at least a computer in communication with the communication network using security data stored internal to the portable data storage device.

24. A method of backing up data of a key-server in communication with a communication network as defined in claim 23 wherein the security data stored internal to the portable data storage device are not accessible from outside of the key-server and the portable data storage device.

25. A method of backing up data of a key-server in communication with a communication network as defined in claim 15 wherein the key-server provides dedicated cryptographic functions for the at least a computer in communication with the communication network using security data stored internal to the key-server.

26. A method of backing up data of a key-server in communication with a communication network as defined in claim 25 wherein the security data stored internal to the key-server are not accessible in a useable from outside of the key-server and the portable data storage device.

27. A method of authenticating an individual for allowing access to secure data or secure keys stored on a communication network when other than in communication with a central key-server comprising the steps of:

providing at least a computer in communication with the communication network;

determining at least an available user information entry device from a plurality of known user information entry devices;

determining the availability of one of a key-server and a portable data storage device in communication with the computer;

receiving user identification information via the at least an available user information entry device;

authenticating the individual for access to at least one of the secure data and secure keys stored on the determined one of a key-server and a portable data storage device.

28. A method as defined in claim 27 wherein when a portable data storage device is present the determined one of a key-server and a portable data storage device is the portable data storage device and the received user identification information is registered against user identification information stored in the memory means of the portable data storage device.

29. A method as defined in claim 28 comprising the steps of:
receiving unique user identification information via the at least an available user information entry device;
registering the received user identification information against security data for that user stored in the portable data storage device; and,
providing secure keys to the user to allow access to encrypted data files that the user has been authenticated to access.

30. A method as defined in claim 28 comprising the steps of:
receiving unique user identification information via the at least an available user information entry device;
registering the received user identification information against security data for that user stored in the portable data storage device; and,
providing cryptographic functions within the portable data storage device using the secure keys associated with the authenticated user.

31. A method as defined in claim 28 wherein when a portable data storage device is other than present prompting the user to provide a portable data storage device.

32. A method as defined in claim 28 wherein other than when the user provides a portable data storage device a key-server in communication with the communication network is the determined one of a key-server and a portable data storage device.

33. A method as defined in claim 32 comprising the steps of:
receiving unique user identification information via the at least an available user information entry device;
registering the received user identification information against security data for that user stored in the key-server; and,
providing secure keys to the user to allow access to encrypted data files that the user has been authenticated to access.

34. A method as defined in claim 32 comprising the steps of:
receiving unique user identification information via the at least an available user information entry device;
registering the received user identification information against security data for that user stored in the key-server; and,
providing cryptographic functions within the key-server using the secure keys associated with the authenticated user.

35. A method as defined in claim 31 wherein the portable data storage device is one of a smart card and a PCMCIA token

36. A method as defined in claim 35 wherein the portable data storage device in the form of a PCMCIA token provides dedicated cryptographic functions for the computer using security data stored internal to the PCMCIA token.

37. A method as defined in claim 36 wherein the security data stored internal to the PCMCIA token are not accessible from outside of the PCMCIA token and therefore cannot be extracted or otherwise read by an unauthorized third party.

38. A method as defined in claim 32 wherein the user information entry device is a biometric information entry device.

39. A method as defined in claim 31 wherein a portable data storage device is used to provide an individual with access to a predetermined set of keys in a plurality of different locations.

40. A method as defined in claim 39 wherein the method of user authentication required at work is other than the method of user authentication required elsewhere.

41. A method as defined in claim 27 wherein the portable data storage device provides dedicated cryptographic functions for the computer using security data stored internal to the portable data storage device.

42. A method as defined in claim 41 wherein the security data stored internal to the portable data storage device are not accessible in a useable from outside of the key-server and the portable data storage devices.

43. A method as defined in claim 27 wherein the key-server provides dedicated cryptographic functions for the computer using security data stored internal to the key-server.

44. A method as defined in claim 43 wherein the security data stored internal to the key-server are not accessible from outside of the key-server and the portable data storage devices.